R E P U B L I Q U E F R A N C A PCT/FR 98/02753

FR 98/02753

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

REC'D 18 JAN 1999
WIPO PCT

EJV

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

09/581646

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 22 DEC. 1998

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : (1) 42.94.52.52 Télécopie : (1) 42.93.59.30

BREVET D'INVENTION, CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle-Livre VI

cerfa N° 55-1328

REQUÊTE EN DÉLIVRANCE

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES 16/12/97

N° D'ENREGISTREMENT NATIONAL 97 15971

DÉPARTEMENT DE DÉPÔT 75

DATE DE DÉPÔT 16 DEC. 1997

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

SCHLUMBERGER INDUSTRIES
Transactions Electroniques
50 Av. Jean Jaurès - B.P 620-04
92542 MONTROUGE Cédex
A l'attention de Christophe MACQUET

n°du pouvoir permanent PG06273 | références du correspondant 76-459 | téléphone 01 47 46 63 72

2 DEMANDE Nature du titre de propriété industrielle

☒ brevet d'invention ☐ demande divisionnaire ☐ certificat d'utilité ☐ transformation d'une demande de brevet européen

demande initiale ☐ brevet d'invention ☐ certificat d'utilité n° date

Établissement du rapport de recherche ☐ différé ☒ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance ☐ oui ☐ non

Titre de l'invention (200 caractères maximum)

PROCEDE DE SECURISATION DE LA TRANSMISSION D'UN MESSAGE D'UN DISPOSITIF EMETTEUR A UN DISPOSITIF RECEPTEUR

3 DEMANDEUR (S) n° SIREN 542062120 code APE-NAF

Nom et prénoms (souligner le nom patronymique) ou dénomination

Schlumberger Industries

Forme juridique

Société Anonyme

Nationalité (s) Française

Adresse (s) complète (s) Pays

50, Avenue Jean Jaurès
92120 MONTROUGE

France

En cas d'insuffisance de place, poursuivre sur papier libre ☐

4 INVENTEUR (S) Les inventeurs sont les demandeurs ☐ oui ☒ non Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES ☐ requise pour la 1ère fois ☐ requise antérieurement au dépôt ; joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine	numéro	date de dépôt	nature de la demande
SANS			

7 DIVISIONS antérieures à la présente demande n° date n° date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE
(nom et qualité du signataire - n° d'inscription)

Christophe MACQUET
Mandataire
(PG06273)

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION

SIGNATURE APRES ENREGISTREMENT DE LA DEMANDE À L'INPI

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION, CERTIFICAT D'UTILITE

DÉSIGNATION DE L'INVENTEUR
(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

DIVISION ADMINISTRATIVE DES BREVETS

26bis, rue de Saint-Pétersbourg
75800 Paris Cédex 08
Tél. : (1) 42 94 52 52 - Télécopie : (1) 42 93 59 30

76-459

N° D'ENREGISTREMENT NATIONAL

97 15 971

TITRE DE L'INVENTION :

PROCEDE DE SECURISATION DE LA TRANSMISSION D'UN MESSAGE D'UN DISPOSITIF EMETTEUR A UN DISPOSITIF RECEPTEUR

LE (S) SOUSSIGNÉ (S)

Christophe MACQUET
SCHLUMBERGER INDUSTRIES
Transactions Electroniques
50, avenue Jean Jaurès - BP 620-04
92542 MONTROUGE Cédex

DÉSIGNE (NT) EN TANT QU'INVENTEUR (S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

BRAHAMI Lionel
26, place Jules Ferry
92120 MONTROUGE
France

RIGAL Vincent
40, avenue de la Gare
92330 SCEAUX
France

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

Le 16 décembre 1997

Christophe MACQUET
(PG 06273)

PROCEDE DE SECURISATION DE LA TRANSMISSION D'UN MESSAGE D'UN DISPOSITIF EMETTEUR A UN DISPOSITIF RECEPTEUR

L'invention concerne un procédé de sécurisation de la transmission de messages d'un dispositif émetteur à un dispositif récepteur.

Lorsqu'une information est transmise d'un dispositif émetteur à un dispositif récepteur, cette information, contenue dans un message, est susceptible d'être altérée au cours de sa transmission. Cette altération peut provenir soit, d'un défaut dans l'émission, la transmission ou la réception du message soit, d'une fraude d'un tiers. Le message reçu n'est alors pas intègre.

C'est la raison pour laquelle on a développé des procédés qui permettent de vérifier l'intégrité des messages transmis.

Par ailleurs, lorsqu'une information est transmise d'un dispositif émetteur à un dispositif récepteur, il est parfois utile de rendre le message confidentiel de manière à réserver l'accès de ladite information à un nombre limité de personnes, en général l'émetteur et le récepteur du message.

C'est la raison pour laquelle on a développé des procédés permettant de préserver la confidentialité d'un message.

Enfin, lorsqu'une information contenue dans un message est transmise à un dispositif récepteur, il est bien souvent utile d'authentifier ce message comme provenant effectivement du dispositif émetteur.

C'est la raison pour laquelle on a développé des procédés d'authentification des messages.

Les procédés connus de vérification de l'intégrité, de préservation de la confidentialité et d'authentification, c'est-à-dire de sécurisation des messages, consistent généralement à crypter le message et à lui joindre un certificat avant sa transmission. Le dispositif récepteur décrypte alors le message, vérifie le certificat et, éventuellement, dans le cas où ledit message est un programme informatique, l'exécute.

Ces procédés présentent une évidente lourdeur, dans la mesure où le décryptage et la vérification du certificat imposent chacune une opération. C'est le cas, en particulier, lorsque les opérations de cryptage et de décryptage sont longues.

Considérant ce qui précède, un problème que se propose de résoudre l'invention est de réaliser un procédé de sécurisation de la transmission d'un message d'un dispositif émetteur à un dispositif récepteur qui ne nécessite pas la mise en oeuvre des deux étapes précitées de décryptage du message et de vérification du certificat.

Eu égard au problème posé ci-dessus l'invention a pour objet un procédé de sécurisation de la transmission d'un message d'un dispositif émetteur à un dispositif récepteur, caractérisé en ce que :

- le message est divisé en n unités élémentaires, n étant un nombre supérieur ou égal à 1 ;

- une propriété logique est définie de manière que, pour toute unité élémentaire, la propriété logique, appliquée à une unité élémentaire authentique, donne une valeur logique du type vrai ;

- le message est crypté par des moyens de cryptage du dispositif émetteur à l'aide d'un algorithme de cryptage comportant

une clé de manière à obtenir un résultat crypté ;

- le résultat crypté est transmis par le dispositif émetteur au dispositif récepteur ;

- le résultat crypté est décrypté par le dispositif récepteur à l'aide d'un algorithme de décryptage comportant une clé secrète de manière à obtenir un résultat décrypté ;

- le résultat décrypté est divisé en unités élémentaires ;

- la propriété logique est appliquée aux unités élémentaires de manière à obtenir, pour chaque unité, une valeur logique du type vrai ou du type faux.

- le message est considéré comme authentique et intègre si, pour chaque unité, les valeurs logiques ont une valeur du type vrai.

Le message est alors avantageusement stocké.

On notera par ailleurs que, de manière avantageuse, le message Prgm est un programme informatique susceptible d'être exécuté et/ou d'être interprété par le dispositif récepteur R. Les unités élémentaires sont des instructions du programme Prgm. La propriété P, appliquée à une unité élémentaire I, donne une valeur logique de type vrai lorsque l'unité élémentaire I est exécutable et/ou interprétable. La propriété P, appliquée à une unité élémentaire I, donne une valeur logique de type faux lorsque l'unité élémentaire I n'est pas exécutable et/ou interprétable. Le dispositif récepteur R est un objet portable à mémoire du type carte à puce. Le dispositif récepteur R comporte un objet portable à mémoire du type carte à puce. L'objet portable à mémoire est un module d'identification abonné (SIM). Le message Prgm est écrit dans un langage interprété

de haut niveau. Le langage de haut niveau est le langage Java. Le programme informatique est formé d'un ensemble d'instructions précompilées. Le message Prgm est crypté en flux continu ou en blocs chaînés. Le message Prgm est crypté en blocs et en ce que les blocs du message Prgm crypté sont permutés. Un des blocs permutés est un bloc de début ou de fin du message Prgm. Le résultat Kc(Prgm) est décrypté par blocs, chaque bloc crypté étant à l'origine d'un bloc décrypté prenant la place du bloc crypté. Les algorithmes de cryptage et de décryptage font intervenir un aléa, transmis par le dispositif émetteur E, au dispositif récepteur R. Le message Prgm est enregistré, après vérification, dans une mémoire non volatile du dispositif récepteur R.

Cette invention sera mieux comprise à la lecture de la description non limitative qui va suivre.

Selon l'invention, le message Prgm est transmis d'un dispositif émetteur E à un dispositif récepteur R.

Le message Prgm est par exemple un programme informatique susceptible d'être exécuté et/ou interprété.

Le dispositif émetteur E est, par exemple, un serveur, un ordinateur, une station émettrice dans un réseau de télécommunication ou un lecteur de cartes à puce avec ou sans contact, bref, tout dispositif capable de crypter et d'émettre un message. Bien entendu, le dispositif émetteur E doit être considéré dans un sens large comme incluant des dispositifs complexes formés notamment de parties physiquement séparées, une partie assurant par exemple le cryptage du message, une autre, l'émission stricto sensu dudit message.

Le dispositif récepteur R est, par exemple, un ordinateur éventuellement muni d'un lecteur de carte à puce et d'une carte insérée dans ledit lecteur, une station réceptrice dans un réseau de télécommunication, un téléphone portable muni ou non d'un module d'identification abonné (SIM) voire même une carte à puce ou un tel module, bref, tout dispositif capable de recevoir un message voire de stocker ce message et, avantageusement, lorsque le message est un programme informatique, d'interpréter et/ou d'exécuter ce programme. Dans le cas où le dispositif récepteur comporte avantageusement un objet portable à mémoire du type carte à puce, cet objet portable peut être une carte de paiement ou une carte de contrôle d'accès, par exemple, à un réseau informatique.

Dans la suite de l'exposé de l'invention, on se limitera aux exemples où le message est un programme informatique Prgm.

Selon l'invention, ce programme informatique Prgm est divisé en n unités élémentaires I, n étant un nombre entier supérieur ou égal à 1. Il s'agit d'instructions, de blocs d'instructions ou, dans le cas où le programme Prgm est rédigé dans un langage interprétable du type Java, d'instructions précompilées du programme (ou bytecodes).

Selon l'invention, une propriété logique P est définie de manière que, pour toute unité élémentaire I, cette propriété P, appliquée à une unité élémentaire authentique, donne une valeur logique P(I) du type vrai. On cherchera néanmoins à trouver une propriété P qui, appliquée à une unité élémentaire I, donne une valeur logique P(I) du type faux lorsque ladite unité élémentaire I à été modifiée et correspond par exemple à une instruction non

reconnaissable du programme, notamment non susceptible d'être interprétable et/ou exécutable.

Selon l'invention, le programme Prgm est crypté par des moyens de cryptage du dispositif émetteur E à l'aide d'un algorithme de cryptage comportant une clé Kc connue dudit dispositif E de manière à obtenir un résultat Kc(Prgm). Le cryptage garantit la confidentialité du programme Prgm lors de son émission et de sa réception, mais, surtout, durant sa transmission au dispositif récepteur R. Ce résultat Kc(Prgm) est alors transmis par le dispositif E, au dispositif récepteur R.

Il est ensuite décrypté par ce dispositif R à l'aide d'un algorithme de cryptage comportant une clé secrète Kd, connue du dispositif récepteur. Un résultat décrypté Kd(Kc(Prgm)) est alors obtenu.

Cette clé Kc peut être propre au dispositif E et connue du dispositif R, ou propre au dispositif R et par ailleurs connue du dispositif E. Un exemple de la première configuration est le cas où le dispositif R est abonné à un service délivré par le dispositif émetteur. Un exemple de la seconde configuration est le cas où le dispositif récepteur, lors de sa requête d'une transmission du programme, fournit la clé Kc, la clé Kd de décryptage restant connue du seul dispositif récepteur. Un autre exemple de la même configuration est le cas où Kc et Kd sont identiques (système à clé privée), et où cette clé est envoyée, sous forme cryptée, par le dispositif récepteur, au dispositif émetteur.

Selon l'invention, le résultat décrypté Kd(Kc(Prgm)) est divisé ou décomposé en n unités élémentaires, images des ou correspondant

aux n unités élémentaires résultant de la division du programme Prgm dans le dispositif émetteur E.

La propriété logique P est alors appliquée auxdites n unités élémentaires de manière à obtenir, pour chaque unité, une valeur logique du type vrai ou du type faux.

Dans le cas où toutes les valeurs logiques sont du type vrai, on a une forte probabilité que le programme décrypté soit identique au programme crypté et que la clé ayant servi au cryptage soit la clé Kc attendue. Le dispositif récepteur R en déduit alors que le programme Prgm est intègre et qu'il a été émis par un dispositif émetteur E disposant de la clef Kc, donc authentique.

Par contre, dans le cas où une valeur logique au moins est du type faux, le programme décrypté est différent de Prgm et le dispositif récepteur R en déduit que le programme Prgm a fait l'objet d'au moins une modification à l'émission, à la réception ou durant sa transmission et/ou que ledit programme Prgm a crypté le message avec une clé autre que Kc, une clé non attendue. Le programme est n'est alors pas intègre ou pas authentique.

L'invention permet donc de garantir, en une seule opération de cryptage-décryptage, à la fois l'intégrité, l'authentification et la confidentialité du programme Prgm.

Si l'on considère par exemple que les instructions du langage informatique dans lequel est rédigé le programme Prgm sont des instructions codées sur quatre octets, il y a, en théorie, 2^{32} codes possibles pour définir une instruction. Bien entendu, certains codes, définis par un ensemble de paramètres, ne correspondent à aucune instruction compréhensible. De plus, certains paramètres de certains

codes, typiquement les trois derniers octets, n'ont que certaines valeurs autorisées. Une adresse mémoire ne peut ainsi être négative, ou se situer en dehors de l'espace alloué au programme Prgm. C'est la raison pour laquelle la propriété P comporte un avantageusement un test de paramètres, ledit test dépendant du type d'instruction.

Si l'on définit le taux de non-détection unitaire C comme étant le pourcentage des instructions possibles qui ne sont pas reconnues comme fausses par l'application de la propriété P lors du décryptage et suite à une modification ponctuelle du programme Prgm, la probabilité que le dispositif récepteur R ne détecte pas la fraude est, lorsque la modification ponctuelle est à l'origine d'une modification sur chaque instruction du résultat décrypté :

$$prob = (1 - C)^n.$$

Pour les valeurs typiques suivantes, on obtient les probabilités prob suivantes :

n	C (%)	prob
256	10%	1.9E-12
128	10%	1.4E-06
512	5%	3.9E-12
128	5%	1.4E-03

On constate que la probabilité qu'une modification notamment frauduleuse passe inaperçue est très faible, sauf dans les cas de programmes comportant peu d'instructions et dont le taux de non-détection unitaire C est très élevé. Cette probabilité est a fortiori très faible dans le cas où le programme a été crypté par une clé autre que Kc.

Comparée aux opérations de cryptage usuelles, l'application de la propriété P ne nécessite pas une mise en oeuvre trop lourde

notamment un temps de calcul trop long. Elle permet la détection des erreurs dans tous les types de programmes Prgm dès lors que l'algorithme de cryptage est de bonne qualité, eu égard au caractère pseudo-aléatoire de tout décryptage d'une suite d'instructions falsifiées.

L'algorithme de cryptage est avantageusement du type en blocs chaînés ou en flux continu. Ainsi, une modification d'une instruction élémentaire entraînera une modification d'autres instructions. Par contre, lorsque l'algorithme procède uniquement par blocs, le programme crypté peut être décomposé en une suite de par exemple n blocs correspondant peu ou prou aux n unités élémentaires. En modifiant un bloc et en observant le comportement du dispositif récepteur, la probabilité prob que la modification ne soit pas détectée est alors est égale à 1 - C, donc très élevée.

De manière à éviter une modification dirigée sur le bloc de tête ou de queue du programme crypté, on permute, par exemple, les blocs du programme crypté, de manière que lesdits blocs de tête et de queue du programme soient à un endroit qui ne soit pas prédictible par un fraudeur, mais néanmoins connu des dispositifs E et R.

La confidentialité est par ailleurs améliorée lorsque l'algorithme de cryptage fait intervenir un aléa généré par exemple par le dispositif récepteur R et communiqué au dispositif émetteur E. Il peut s'agir, par exemple, d'une opération "ou exclusif" appliquée sur un nombre d'octets déterminé du programme ou sur sa totalité avant cryptage.

On pourra enfin introduire en début et/ou en fin de programme, avant cryptage, des instructions vides (NOP), que le

dispositif récepteur reconnaîtra en appliquant la propriété P, puis éliminera.

Dans un premier mode de mise en oeuvre de l'invention, le dispositif émetteur E est une station de base d'un réseau de télécommunication GSM (Global System for Mobil communication) ou de tout autre système de téléphonie mobile faisant intervenir un module de sécurité, le dispositif récepteur R est un module d'identification abonné SIM associé à un téléphone mobile. Le programme Prgm, destiné à être téléchargé dans ledit module SIM, est codé sous la forme d'instructions précompilées (bytecodes) rédigées par exemple dans le langage Java.

Bien entendu, l'invention s'applique de la même manière aux d'autres systèmes à cartes à puces, tels que des systèmes de paiement ou de contrôle d'accès.

Dans ce premier mode de mise en oeuvre de l'invention, le programme est divisé en n unités élémentaires, une unité élémentaire étant une instruction précompilée d'un nombre de bits déterminé (fixe ou dépendant du type d'instruction).

La propriété logique P est définie de manière qu'elle prenne une valeur logique vrai lorsque l'unité élémentaire à laquelle elle est appliquée est une instruction exécutable (ou interprétable) ou correspond à une instruction NOP.

Le programme Prgm est alors crypté par le dispositif émetteur E avec un algorithme de cryptage, par exemple du type RSA (Rivest, Shamir et Adelman) tel que décrit dans le brevet US-4,405,829. Un résultat de cryptage Kc(Prgm), fonction de la clé Kc, est alors obtenu.

Ce résultat Kc(Prgm), en définitive le programme crypté, est transmis par la station de base à une station émettrice qui lui est associée puis à des moyens de réception du téléphone mobile. Il est alors chargé dans la carte où il est enregistré dans une mémoire non volatile EEPROM avant l'opération de décryptage, compte tenu de la lenteur de cette opération mise en oeuvre sur un module SIM.

Le résultat Kc(Prgm) est ensuite décrypté à l'aide d'un algorithme de décryptage comportant une clé secrète Kd. Chaque bloc du résultat décrypté est enregistré dans la mémoire non volatile EEPROM du module SIM, à l'adresse du bloc du résultat crypté correspondant. Ainsi, l'espace mémoire utilisé pour la mise en oeuvre du décryptage selon l'invention est minimal. On notera que, dans une variante de mise en oeuvre de l'invention, à l'aide d'au moins un espace mémoire libre correspondant à un bloc, on peut enregistrer les blocs du résultat décrypté à des adresses mémoire différentes des blocs cryptés auxquels ils correspondent. Une permutation circulaire est tout aussi possible, améliorant la sécurisation du programme durant l'étape de décryptage.

L'application de la propriété P s'effectue de préférence à la fin du décryptage complet du résultat crypté Kc(Prgm), le résultat final (programme accepté ou refusé) n'étant donné qu'à la fin de toutes les vérifications. Ainsi, le fraudeur ne peut pas détecter simplement l'unité élémentaire I reconnue comme donnant une valeur logique fausse lors de l'application de la propriété P.

Compte tenu de la faible mémoire disponible dans le module SIM, une fonction de calcul simple de la propriété P est mise en oeuvre. Il s'agit d'une fonction mise en oeuvre par l'interprèteur lui-

même. Une fois que le résultat crypté est décrypté, l'interprèteur interprète le résultat décrypté en regardant si les instructions ont un sens ou non. En définitive, l'interpréteur effectue l'analyse du programme comme il le ferait lors d'une interprétation normale, sans toutefois que ladite interprétation soit suivie d'effet autre que la vérification que le résultat décrypté correspond bien à un programme Prgm.

Dans un second mode de mise en oeuvre de l'invention, le dispositif émetteur E est un serveur comportant une forme précompilée et cryptée Kc(Prgm) d'un programme Prgm, rédigé par exemple dans le langage Java. Le dispositif récepteur R est un ordinateur personnel, qui sera utilement muni d'un lecteur de carte à puce dans lequel est insérée une carte. L'ordinateur personnel comporte un disque dur et une zone mémoire sûre, c'est-à-dire qui n'est pas susceptible d'être lue ou écrite par un tiers, pour le stockage, temporaire ou définitif, des résultats décryptés Kd(Kc(Prgm)) et des clés. L'ordinateur comprend par ailleurs un logiciel de chargement des programmes Prgm appelé Loader invoqué chaque fois qu'il est nécessaire de charger un programme Prgm précompilé, avant que ledit programme Prgm soit utilisé (interprété ou exécuté). Dans le présent second mode de mise en oeuvre de l'invention, ce logiciel inclut une fonction de décryptage, qui comporte avantageusement des éléments fonctionnels nécessaires au décryptage et notamment des éléments de l'algorithme de décryptage. Le logiciel de chargement des programmes est alors dit surchargé. Bien entendu, d'autres éléments fonctionnels nécessaires au décryptage peuvent être contenus dans une mémoire non volatile de la carte à puce. Ces éléments seront

alors appelés par le logiciel de chargement des programmes et la fonction de décryptage. Ainsi, le logiciel de chargement permet, en association avec la carte, le décryptage du résultat Kc(Prgm) et la vérification du résultat décrypté Kd(Kc(Prgm)) avant l'interprétation dudit résultat décrypté Kd(Kc(Prgm)), c'est-à-dire, lorsque la propriété P a été appliquée avec succès, le programme Prgm, et l'exécution de ce programme Prgm.

Les contraintes de temps et d'espace mémoire qui ont été évoquées lors de la description du premier mode de mise en oeuvre du procédé de l'invention sont, dans ce second mode de mise en oeuvre, moindres, étant donné que la carte est ici uniquement utilisée comme un support physique sécurisé d'une ou plusieurs clés ou éléments, des tables par exemple, nécessaires au décryptage. La carte peut même contenir la totalité de l'algorithme secret de décryptage.

La propriété P peut, de ce fait, être non seulement du type de celle précité, ou alors, être une propriété particulière dont on implémentera l'algorithme de vérification. L'algorithme de vérification vérifie dans un exemple les instructions précompilées à chaque fois qu'un bloc instruction(s) du résultat crypté est décrypté.

Les phases d'échange entre, d'une part, l'ordinateur personnel muni de l'interprèteur, du dispositif de chargement et associé à un lecteur de carte dans lequel est inséré la carte et, d'autre part, la carte, peuvent se décomposer en trois phases : une phase d'initialisation, une phase de transfert et une phase de décryptage/vérification.

La phase d'initialisation est en fait une phase d'échange d'un couple de clés publique et secrète. Cette phase est lancée lors de

l'initialisation du processus de décryptage. Les couples de clés ne sont pas écrits sur le disque dur de l'ordinateur personnel et peuvent faire l'objet d'un nouveau calcul à tout moment. Durant cette phase, un ordre de ré-initialisation est transmis par l'ordinateur personnel à la carte. L'ordinateur calcule alors un couple clé publique PKc - clé secrète PKd, puis calcule une signature de la clé publique PKc à l'aide de la clé secrète PKd. Cette signature est transmise, avec la clé publique PKc, vers la carte. Elle est ensuite vérifiée par la carte, à l'aide de la clé publique PKc. La carte calcule alors, à l'aide d'une clé secrète CKd, une signature de la clé publique CKc. Cette signature est transmise, avec la clé publique CKc, vers l'ordinateur personnel. L'ordinateur vérifie la signature, à l'aide de la clé publique CKc.

La phase de transfert est une phase de chargement d'informations secrètes de la carte dans l'ordinateur personnel. Ces informations permettent à l'ordinateur d'effectuer le décryptage de la forme précompilée et cryptée du programme Prgm. Pour cette phase, l'ordinateur demande à la carte le transfert de la clé secrète de décryptage Kd dont elle dispose dans sa mémoire. La carte crypte cette clé en utilisant la clé PKc, et l'envoie à l'ordinateur. Celui ci décrypte ce message à l'aide de sa clé Kd, et dispose ainsi de la clé Kc. Il lui est alors possible de décrypter le programme Kc(Prgm), pour obtenir un programme Prgm', qui n'est autre que le programme originel Prgm si aucune tentative de fraude n'a eu lieu.

L'ordinateur peut à ce moment décomposer le programme Prgm' en unités élémentaires, et leur appliquer la propriété P, comme dans le premier mode de réalisation. Si le résultat est satisfaisant, il archive ledit programme, par exemple sur son disque dur. Il peut

également calculer une information de vérification (par exemple un cheksum ou, mieux, un hashing) et l'archiver dans la mémoire de la carte, à des fins de vérification ultérieures d'intégrité du programme.

REVENDICATIONS

1. Procédé de sécurisation de la transmission d'un message Prgm d'un dispositif émetteur E à un dispositif récepteur R, caractérisé en ce que :

- le message Prgm est divisé en n unités élémentaires I, n étant un nombre supérieur à 1 ;

- une propriété logique P est définie de manière que, pour toute unité élémentaire I, la propriété logique P, appliquée à une unité élémentaire I authentique, donne une valeur logique du type vrai ;

- le message Prgm est crypté par des moyens de cryptage du dispositif émetteur E à l'aide d'un algorithme de cryptage comportant une clé Kc de manière à obtenir un résultat crypté Kc(Prgm) ;

- le résultat crypté Kc(Prgm) est transmis par le dispositif émetteur E au dispositif récepteur R ;

- le résultat crypté Kc(Prgm) est décrypté par le dispositif récepteur R à l'aide d'un algorithme de décryptage comportant une clé secrète Kd de manière à obtenir un résultat décrypté Kd(Kc(Prgm)) ;

- le résultat décrypté Kd(Kc(Prgm)) est divisé en unités élémentaires I ;

- la propriété logique P est appliquée aux unités élémentaires I de manière à obtenir, pour chaque unité, une valeur logique du type vrai ou du type faux ;

- le message Prgm est considéré comme authentique et intègre si, pour chaque unité, les valeurs logiques ont une valeur du type

vrai.

2. Procédé selon la revendication précédente, caractérisé en ce que le message Prgm est un programme informatique susceptible d'être exécuté et/ou d'être interprété par le dispositif récepteur R.

3. Procédé selon la revendication précédente, caractérisé en ce que les unités élémentaires sont des instructions du programme Prgm.

4. Procédé selon la revendication 2 ou 3, caractérisé en ce que la propriété P, appliquée à une unité élémentaire I, donne une valeur logique de type vrai lorsque l'unité élémentaire I est exécutable et/ou interprétable.

5. Procédé selon l'une des revendications 2, 3 ou 4, caractérisé en ce que la propriété P, appliquée à une unité élémentaire I, donne une valeur logique de type faux lorsque l'unité élémentaire I n'est pas exécutable et/ou interprétable.

6. Procédé selon l'une des revendications précédentes, caractérisé en ce que le dispositif récepteur R est un objet portable à mémoire du type carte à puce.

7. Procédé selon l'une des revendications 1 à 5, caractérisé en ce que le dispositif récepteur R comporte un objet portable à mémoire du type carte à puce.

8. Procédé selon la revendication 6, caractérisé en ce que l'objet portable à mémoire est un module d'identification abonné SIM.

9. Procédé selon l'une des revendications précédentes, caractérisé en ce que le message Prgm est écrit dans un langage interprété de haut niveau.

10. Procédé selon la revendication 9, caractérisé en ce que le langage de haut niveau est le langage Java.

11. Procédé selon l'une des revendications 9 ou 10, caractérisé en ce que le programme informatique est formé d'un ensemble d'instructions précompilées.

12. Procédé selon l'une des revendications précédentes, caractérisé en ce que le message Prgm est crypté en flux continu ou en blocs chaînés.

13. Procédé selon l'une revendications précédentes, caractérisé en ce que le message Prgm est crypté en blocs et en ce que les blocs du message Prgm crypté sont permutés.

14. Procédé selon la revendication 13, caractérisé en ce que un des blocs permutés est un bloc de début ou de fin du message Prgm.

15. Procédé selon l'une des revendications 1 à 12, caractérisé en ce que le résultat Kc(Prgm) est décrypté par blocs, chaque bloc crypté étant à l'origine d'un bloc décrypté prenant la place du bloc crypté.

16. Procédé selon l'une des revendications précédentes, caractérisé en ce que les algorithmes de cryptage et de décryptage font intervenir un aléa, transmis par le dispositif émetteur E, au dispositif récepteur R.

17. Procédé selon l'une des revendications précédentes, caractérisé en ce que le message Prgm est enregistré, après vérification, dans une mémoire non volatile du dispositif récepteur R.